Gävle KOMMUN

24AFN223, 24SON196, 24ON471

Årsrapport informationssäkerhetsarbete 2024

Redogörelse för informationssäkerhetsarbetet inom Välfärd Gävle

2025-01-08

Förord

Denna årsrapport redogör övergripande för informationssäkerhetsarbetet inom sektor Välfärd, Gävle kommun. En stor del av informationssäkerhetsarbetet sker i det dagliga arbetet i linjeorganisationen. Den här rapporten tar snarare fokus på de andra operativa och strategiska insatser som sker från centralt håll hos Välfärd Gävle. Rapporten innehåller även information om händelser i vår omvärld som kan vara till stöd för sektor Välfärds kommande beslut kring informationssäkerhet.

2025-01-08

Anita Härdelin
Informationssäkerhetssamordnare
Välfärd Gävle

Innehåll

Inledning

Kommunfullmäktige har beslutat om en policy för informationssäkerhet som säger att kommunens verksamheter ska bedriva ett systematiskt informationssäkerhetsarbete. Viss verksamhet i sektor Välfärd, hälso- och sjukvård, omfattas även av EU-direktivet Network Information Security, NIS samt nationell lagstiftning i form av Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Arbetet med att etablera systematiskt informationssäkerhetsarbete inom sektor Välfärd startade 2022 genom att en informationssäkerhetssamordnare (ISS) tillsattes. Hen har under 2024 arbetat med informationssäkerhet och i nära samarbete med dataskyddssamordnare (DSS) samt vid behov av stöd med kommunens övergripande informationssäkerhetssamordnare (CISO).

Målsättningen med denna årsrapport är att beskriva vad vi hittills har åstadkommit men också belysa viktiga aktiviteter som behöver prioriteras i det fortsatta arbetet.

Om informationssäkerhetsarbetet inom Välfärd Gävle

Vid start av 2022 bemannades rollen som ISS vid Välfärd Gävle. Arbetet med att etablera ett systematiskt informationssäkerhetsarbete för sektorns verksamheter och implementera den svenska lagstiftningen från 2018 utifrån NIS-direktivet påbörjades av ISS med stöd av CISO. Arbetet under 2024, med fortsatt etablering och tillämpning av arbetssätt har skett mer och mer självständigt av Informationssäkerhetssamordnare och vid behov med stöd av CISO. ISS har under året deltagit i flera digitala utbildningar och seminarier i syfte att öka kompetensen på området för sektor Välfärd.

En ny Dataskyddssamordnare (DSS) tillträdde i början på 2024 och ett gott samarbete har utvecklats.

För det systematiska informationssäkerhetsarbetet tillämpas en ledningsmodell framtagen av Myndigheten för samhällsskydd och beredskap (MSB). Del ett, Identifiera och analysera har slutförts tidigare år och delarna två och tre, Utforma och Använda pågår med avslutade och pågående aktiviteter som redovisas längre fram i rapporten.

Omvärldsbevakning

Cybersäkerhet

Cyberhoten har kommit för att stanna och enligt Säpo kommer de att öka. Säpo: Cyberhoten mot Sverige kommer bara att öka | Computer Sweden. Rysslands militära aggression mot Ukraina har förändrat hotbilden i Europa även under 2024 och antalet försök till attacker ökar, även från andra nationer som Iran och Kina. Ett exempel är, som säkerhetspolisen skriver att Sverige används som plattform för främmande makts cyberangrepp. Sverige som plattform för främmande makts cyberangrepp - Säkerhetspolisen. Säkerhetspolisen skriver också om omvärldsutveckling och om NCSC[1]. Cybersäkerhet - Säkerhetspolisen. En rapport från Check Point Research visar att cyberattackerna mot Sverige har under kvartal 3 ökat med 165%. RAPPORT: Cyberattacker i Sverige ökar med 165 procent - Aktuell Säkerhet. En artikel i Computer Sweden i januari 2025 går att läsa om att vården är den sektor som är mest utsatt för cyberhot och att EU nu även arbetar med en handlingsplan. Vården mest utsatt för cyberhot – nu lägger EU fram handlingsplan | Computer Sweden

Informations- och cybersäkerhet står högt upp på den svenska regeringens agenda. Sveriges minister för civilt försvar Carl-Oskar Bohlin (M) har återkommande kommenterar vikten av cybersäkerhetsarbetet. Till exempel, ”Cybersäkerhet utgör en grundpelare i det moderna civila försvaret. I budgetpropositionen för 2025 föreslår regeringen en satsning på 196 miljoner för att stärka informations- och cybersäkerhetsarbetet i det svenska samhället.” Historisk satsning på cybersäkerhet - Regeringen.se och ”I framtiden bör vi dock inte lära oss att leva med hoten om nya attacker, utan i stället minska sårbarheterna, menar ministern för civilt försvar. – Det gäller ända ned på individnivå, att man tar ansvar för sin egen cyberhygien, säger Carl-Oskar Bohlin (M)”. Carl-Oskar Bohlin efter hackerattacken: Ta eget ansvar. Redan när han tillträdde sa han så här ”Cybersäkerhet är en central del av det civila försvaret – inte minst i den säkerhetspolitiska miljö vi befinner oss. Det finns ingen ursäkt för att inte arbeta mycket aktivt och enträget med att skydda sig mot den här typen av angrepp”. Nye ministern om Sveriges cybersäkerhet: ”Alla måste börja göra sitt jobb nu” | Computer Sweden

[1] Nationellt Cyber Säkerhets Center

Likaså står cybersäkerhet högt prioriterat inom Nato och EU. EU beslutade under året om skärpning av NIS[2], så kallad NIS2, som innebär bland annat att fler entiteter ska omfattas samt högre krav[3] på omfattande entiteterna. Europaparlamentet skriver 2023 om de vanligaste och största cyberhoten. Cybersäkerhet: de vanligaste och största cyberhoten | Ämnen | Europaparlamentet. Även NATO skriver om Cyber defence. NATO - Cyber defence.

Cybersäkerhetslagen (NIS2)

”Syfte med NIS2 är att ytterligare bygga upp informations- och cybersäkerhetskapaciteten i hela unionen och utifrån ett **allriskperspektiv begränsa hoten mot nätverk- och informationssystem** som används för att tillhandahålla samhällsviktiga tjänster och **säkerställa kontinuiteten** i sådana tjänster när de **utsätts för incidenter** och därigenom bidra till unionens säkerhet och till att dess ekonomi och samhälle kan fungera effektivt.”

På Myndigheten för samhällsskydd och beredskap (MSB) kan man läsa mer om NIS2. Det här är NIS2-direktivet.

Det återstår en del arbete innan Cybersäkerhetslagen kan beslutas och MSB ge ut förordningar kring hur vi praktiskt kommer att påverkas för att uppfylla lagen. I dagsläget tror man att lagen kommer att gälla från 1 augusti 2025.

Cybersäkerhetslagen kommer även att vara en paketlösning med CER. Syfte med CER är att **minska sårbarheter och stärka den fysiska motståndskraften hos samhällsviktig verksamhet** inom EU för att säkerställa ett oavbrutet tillhandahållande av tjänster som är väsentliga för ekonomin och samhället som helhet samt öka motståndskraften hos den samhällsviktiga verksamhet som tillhandhåller dessa tjänster.

På MSB kan man läsa mer om CER. EU och arbetet med att stärka motståndskraften i samhällsviktig verksamhet.

Den troliga praktiska påverkan på sektor Välfärd vad gäller Cybersäkerhetslagen och som har informerats om av MSB med flera är:

- Cybersäkerhetslagen/NIS2 kommer att omfatta hela sektor Välfärds verksamhet och inte som idag enbart Hälso- och sjukvård.

[2] Network Information Security
[3] Se mer i rubriken Cybersäkerhetslagen (NIS2)

- Incidenthantering och rapportering i större utsträckning med fler IT-leverantörer[4] i och med att hela Välfärds verksamhet omfattas.
- Kontinuitetshantering. Planering, förvaltning och övning av kontinuitet och dess planer för alla sektorns verksamheter.
- Säkerhet i leveranskedjan, vilket innebär att vi behöver följa upp våra leverantörer och dess underleverantörer utifrån deras säkerhet i leveransen av IT. Har vi inte avtal som reglerar kraven behöver nya avtal upprättas.
- Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation. Vilket innebär att vi behöver säkerställa att vi köper in cybersäkra system, applikationer, IT-tjänster.
- Strategier och förfaranden för användning av kryptografi och kryptering vilket vi behöver säkerställa att alla våra IT-leverantörer lever upp till.
- Personalsäkerhet vilket kan innebära att både vår egen personal och våra leverantörers personal har genomgått en bakgrundskontroll
- Strategier för åtkomstkontroll och tillgångsförvaltning vilket vi behöver säkerställa att våra IT-leverantörer lever upp till.
- Säkrade lösningar för kommunikation vilket vi behöver säkerställa att våra IT-leverantörer lever upp till.
- Lösningar för autentisering vilket vi behöver säkerställa att våra IT-leverantörer lever upp till.
- Obligatorisk utbildning för ledningen samt erbjuda alla medarbetare utbildning.
- Högre belopp för vite om Cybersäkerhetslagen inte efterlevs.

[4] Omfattar alla leverantörer av system, applikationer, backup osv inkl SG IT.

Cyberattacker som påverkat Sverige

It-attacken mot Tietoevry It-attacken mot Tietoevry | SVT Nyheter

”Hackergruppen Akira har genomfört en omfattande cyberattack mot den finska IT-leverantören Tietoevry januari 2024. Lönesystemen hos 120 myndigheter har slagits ut, flera regioner och kommuner har fått problem med sina IT-system och även privata företag har drabbats”. Flera drabbade aktörer driver nu skadestånd mot Tietoevry. Regioner kräver Tietoevery på miljoner efter cyberattacken | Computer Sweden

Crowdstrike

”En felaktig uppdatering från cybersäkerhetsföretaget Crowdstrike orsakade ett globalt it-haveri. Detta påverkade allt från flygbolag och banker till svenska trafikbolag. Miljontals Windows-enheter kraschade, vilket resulterade i förseningar och driftstopp över hela världen.14 aug. 2024” Crowdstrike-haveriet – snabb lösning men långsam återhämtning | Computer Sweden

Andra exempel

Malmö stad utsatt för misstänkt cyberattack - Senaste nytt – snabba nyheter från Aftonbladet (4/11)

Kumla kommun utsatt för cyberangrepp - Kumla kommun (4/11)
https://sverigesradio.se/play/artikel/8802976

Cyberattack mot Nordea (25/10)

Bjuv utsatt för hackerattack – utpressas av rysk grupp (27/2)

Hackerattacker och it-störningar – flera aktörer drabbade (5/3)

Umeå universitet utsatt för omfattande cyberattack (2/5)

Regional särskild sjukvårdsledning med anledning av cyberattack mot Sophiahemmet - Nyheter - Region Stockholm (28/2)

Leksands kommun utsatt för IT-attacker och inbrott - Siljan News (19/9)

Effekter av IT-angreppet 6 februari - Kalmar

IT-attacken som drabbat Vellinge kommun får mycket stora följder — Vellinge kommun (19/1)

Störningar på grund av IT-attack | Bjurholm kommun (13/5)

Cyberangrepp mot Norrmejerier i Umeå – produktionen nere | SVT Nyheter (16/4)

Västerås stad under it-attack - P4 Västmanland | Sveriges Radio (26/11)

Surahammars kommun utsatt för cyberangrepp - P4 Västmanland | Sveriges Radio (29/11)

Med flera…

Verksamhet under året

Operativt arbete

Riskanalyser har genomförts i samband med informationsklassningar och konsekvensbedömningar.

Årliga riskanalyser har genomförts för informationsbehandling i 5 system där konfidentialiteten klassats som 2 eller 3.

Stöd vad gäller informationssäkerhetskrav vid upphandlingar av 3 IT-stöd.

Stöd i specifika frågor kring informationssäkerhet samt motsvarande i uppdraget kring ny lagringslösning.

28 informationsklassningar har genomförts under året som lett till åtgärdsplan som överlämnats för genomförande till Informationsägare (chef) och åtgärdsansvarig.

28 incidentrapporter har skrivits och överlämnats till ledningen, nämnd och informations- och/eller systemägare (chef). 4 av dessa avsåg olovlig läsning i Treserva Vo.

0 incidentrapporter till MSB, i enlighet med Lag om samhällsviktiga tjänster. (2018:1174)

Ett stort antal **ringa informationssäkerhetsincidenter**, utifrån brist i konfidentialiteten, har rapporterats tillsammans med incidentrapporteringen för personuppgiftsincident.

3 rapporter från **omvärldsbevakning** har skrivit och delgett Sektorsledningen.

Rapporter, muntligen, sammanställning från utbildning med **rekommendation inför ny lagstiftning** kring NIS2 och CER har genomförts och delgett verksamhetschef och biträdande sektorchef.

Metod för kontinuitetsplanering vid IT-avbrott har anpassats för sektor Välfärd utifrån MSB:s metod.

Stöd inför och under kontinuitetsplanering vid IT-avbrott har gett specifikt till 2 verksamheter samt generellt vid öppna möten vid 2 tillfällen.

Stöd i Informationssäkerhetsklassning i samband med ny lagringslösning har genomförts vid öppna möten en gång per månad under hela 2024.

Stöd, diskussion och utbildning av Komvux Dataskydds- och Informationssäkerhetskoordinator (**DISK**) har genomförts ca vart annan vecka.

Utbildning och information på APT:er och verksamhetsmöten.

Ett antal **rutiner** kring informationssäkert agerande, dokumenterat i Canea One. Frågan kring hur nya rutiner ska informeras till berörda verksamheter har lyfts till ledningen. (kommunikationschef och biträdande sektorchef). Syfte med rutinerna är att vid tillämpandet öka informationssäkerheten. Om de inte är kända i berörda verksamheter kommer de inte att tillämpas och ökad informationssäkerhet uteblir.

Taktiskt arbete

Arbetet i fas 2 och 3 har pågått under hela 2024 och arbete med fas 4 har påbörjats. Dock kvarstår frågor kring hur och vem som ansvarar för att genomföra uppföljning av till exempel genomförandet av åtgärder vid incidenter (Fas 4).

Cybersäkerhetslagen

Inför Cybersäkerhetslagen har två träffar genomförts med CISO för dialog kring vad lagen konkret kommer att innebära för sektor Välfärd.

ISS har deltagit i utbildningar och informationer kring den kommande lagstiftningen samt rapporterat och drivit frågorna internt på sektorn.

Utbildning och informationssäkerhetskultur

Förslag till **utbildningsplan** togs fram 2022 och överlämnades för diskussion och beslut till biträdande sektorchef. Ingen åtgärd under 2024.

Organisation och säkerhetskultur

Förslag till organisation togs fram under 2023 och överlämnades för diskussion till biträdande sektorchef. Två förslag var mest angelägna att få på plats. Dels föreslaget till att **inrätta en styrgrupp** för frågor kring informationssäkerhet och dataskydd. Biträdande sektorchef beslutade att befintlig styrgrupp kring strategiska och operativa IT frågor på sektor Välfärd skulle hantera även dessa frågor och beslut. ISS och DSS deltar i denna styrgrupp. I och med omorganisation skapades en enhet för säkerhet och beredskap där även strategiska frågor hanteras.

Förslaget till att **utse chefstöd**, så kallade DISK:ar i organisationen i syfte att dels stödja chefer (Informationsägare) i deras ansvar för informationssäkerheten inom sin verksamhet, dels som samtalskontakt vid incidenter och registerutdrag och behov av stöd i varje

verksamhet med ISS och DSS har inte genomförts. Dock finns en DISK utsedd i organisationen (Komvux) och som utsågs utifrån eget initiativ. En avgörande framgångsfaktor i att uppnå en acceptabel informationssäkerhetskultur inom sektorn är att etablera en organisation i hela sektorn så kunskap och kompetens kan spridas som ringar på vattnet och därmed bli en naturlig del i det dagliga arbetet på liknande sätt som sekretess. Att ha en organisation med få medarbetare centralt för dessa frågor kommer inte att bidra till en ökad informationssäkerhetskultur i sektorn, vilken är en stor risk för vår möjlighet att skydda vår information som vi har ett stort behov av för att utföra vårt uppdrag tryggt och en välfärd att lita på för våra kunder. Se även resultat av aktivitet i årsrapporten 2023 kring fejkat mejl till chefer.

Cybersäkerhetslagen kommer att ställa krav på att ledningen ska utbildas inom informationssäkerhet samt att all personal ska erbjudas utbildning.

Inköp och upphandling

Frågan kring styrning och kontroll vid inköp av IT relaterade system och applikationer har diskuterats och ett arbete har påbörjat för ett systematiskt arbetssätt under 2024. Dock har arbetet avstannat eftersom ledare av uppdraget erhållit annan tjänst. Ett inköpsstopp infördes under hösten utifrån rekommendation av ISS och DSS och förhoppningen är att när inköpsstoppet hävs finns en fungerande rutin och organisation på plats som säkerställer att IT relaterade inköp är informationssäkra.

Cybersäkerhetslagen kommer att ställa krav på att vi har kontroll på att inköpta system och applikationer är informationssäkra innan vi tar dem i drift varför rekommendationen är att *arbetet prioriteras så att vi följer lagen när den träder i kraft.* Kravet i lagstiftningen kan eventuellt också innebära att vi behöver se över våra befintliga avtal om vi har ställt informationssäkerhetskrav som vi kan följa upp emot. Om vi inte har det rekommenderats att avtal skrivs om.

Uppföljning av IT-leverantörer och dess underleverantörer

Kravet kommer att finnas i Cybersäkerhetslagen vilket kommunicerades redan 2023. Rekommendationen har sen våren 2023 varit att påbörja en dialog kring vem och hur denna uppgift ska genomföras inom sektorn. Rekommendationen är fortfarande att denna uppgift prioriteras så att vi följer lagen när den träder i kraft.

Incidentrapportering

Process och ansvar för incidentrapporteringen internt och till MSB är etablerad och har fungerat bra. I och med Cybersäkerhetslagen kommer rapportering att krävas för alla IT-avbrott i sektorn som uppfyller MSB:s rapporteringskrav. Hur arbetet ska organiseras rekommenderas att diskussion och planering prioriteras.

Ny entitet

En ny entitet i Cybersäkerhetslagen är offentlig förvaltning. Det innebär att all verksamhet omfattas av Cybersäkerhetslagen och inte enbart Hälso- och sjukvård som gällde i NIS.

CER

Parallellt med Cybersäkerhetslagen och som en paketlösning kommer en lag med arbetsnamnet CER som på liknande sätt som Cybersäkerhetslagen syftar till att skydda våra verksamheter från oplanerade avbrott. CER omfattar annat än direkta IT-avbrott dvs fysiska händelser. Dessa två lagar är tänkt att införas på liknande systematiska arbetssätt. Det är oklart för vilka verksamheter CER kommer att gälla för men troligen Hälso- och sjukvård. Rekommendationen är att även frågan kring HUR vi arbetar för att uppfylla CER prioriteras.

Genomförande av åtgärder i syfte att öka informationssäkerheten

Vid informationssäkerhetsklassningar, riskanalyser och incidenter identifieras åtgärder för att minimera eller eliminera risker för att skydda informationen. Dessa åtgärder läggs in i ledningssystemet Stratsys som stöd för genomförandet och för uppföljning.

I skrivande stund finns 240 åtgärder inlagda och av dessa har 92 klarmarkeras och 64 är pågående eller förlängda pga att de förfallit. Det innebär att 52 % av åtgärderna har åtgärdats och därmed bidragit till att ökat informationssäkerheten medan 48 % av åtgärderna inte genomförts utan fortfarande är risker för att informationen inte har tillräckligt skydd. Under 2023 var siffran för klarmarkerade 36% vilket innebär en förbättring.

Biträdande sektorchef har gått ut med information i chefsforum om vikten att genomföra åtgärder som identifierats och godkänts av Informationsägare (chef). Konstaterat är dock att engagemanget att genomföra åtgärder och därmed öka informationssäkerheten fortfarande är lågt. Kanske behöver Informationsägare och andra åtgärdsansvariga få

upplevelsen av ett större avbrott för att få insikten och prioritera informationssäkerhet i sin verksamhet.

Frågan kring vem som ansvarar för att följa upp att åtgärder genomförts är fortfarande oklar. Om vi inte genomför åtgärderna, finns ingen nytta med att rapportera incidenter och arbeta med ständiga förbättringar i syfte att öka skyddet för vår information och därmed våra möjligheter att utföra vårt uppdrag på ett tryggt sätt och en välfärd att lita på för våra medborgare.

Årliga riskanalys

NIS ställer krav på årlig riskanalys för system och nätverk som används för Hälso- och sjukvård. En rekommendation finns också från CISO om att årliga riskanalyser bör genomföras för informationsbehandlingar klassats som en 2: a eller 3: a vad gäller konfidentialiteten. Rutin och tillämpning av rutin för årliga riskanalyser har beslutats. Under året har vi påbörjat att genomföra årliga riskanalyser. Ett års hjul har skapats i Stratsys som stöd för när det är dags för årlig riskanalys för respektive system. Input i riskanalysen är inträffade incidenter under året samt nya insikter kring risker utifrån omvärldsbevakning. Framgent är det tänkt att även resultat från uppföljning av IT leverans, dess leverantörer och underleverantörer samt resultat från uppföljning av Personuppgiftsbiträdesavtal ska vara input i den årliga riskanalysen.

Avrådan

Ingen avrådan har getts under 2024.

Nätverkande och vidareutbildning

ISS har deltagit på:

KIS nätverkets två digitala möten under året. KIS nätverket är ett nationellt nätverk för kommuner. Under nätverkandet erhålls information kring informationssäkerhet och det ges tillfälle att diskutera aktuella frågor med andra kommuner.

CISO:s nätverk för alla verksamheter inom Gävle kommunkoncern inkl bolagen. Även här ges information/utbildning samt möjlighet att diskutera aktuella frågor med andra kommuner.

Ett antal kortare gratis digitala seminarium med MSB, SKR och privata aktörer om Informationssäkerhet, Välfärdsteknik och kommande Cybersäkerhetslag.

Ett digitalt tvådagarsseminarium kring cybersäkerhet anordnat av MSB i Stockholm.

Varje vecka har ISS och DSS samverkat kring informationssäkerhet och dataskydd.

Löpande avstämningsmöten med CISO.

Två möten mellan CISO och biträdande sektorchef kring kommande lagstiftning.

Granskning

Ingen granskning av CISO har genomförts.

Incidenter

Vi har haft 28 incidenter under året. I de allra flesta fallen har orsaken var brist i tillgängligheten genom systemavbrott eller nätverksavbrott på grund av tekniska fel eller mänskliga faktorn.

5 incidenter har förekommit kring TES, varav enbart 1 berodde på teknisk brist och 4 på handhavandebrister.

Tekniska incidenter kring Treserva Vo har haft en positiv utveckling från 12 under 2023 till 2 under 2024. Incidenter kring olovlig läsning i Treserva Vo har noterats till 4 under 2024.

Åtgärdsförslag för att motsvarande incident inte ska hända igen har tagits fram och rapporterats till Informationsägare och ledning.

Det som kan konstateras är att incidenter som skett pga brister hos driftsleverantören SG IT i samband med uppdateringar har minskat rejält vilket är positivt och glädjande för verksamheterna som kunnat genomföra sina uppdrag betydlig tryggare än under 2023.

Även för verksamheten larm är det positivt, som haft ett 2 avbrott sen ny leverantör började gälla. Vid båda avbrotten bör uppmärksammas att leverantören brustit i kommunikationen kring uppdatering och avbrott, trots att de uppgett i upphandlingen att de uppfyller kraven kring kommunikation och samarbete med kunden.

Avbrott och störningar för våra verksamheter som fått större påverkan på dem har varit planerade datorutbyten som inte fungerat tillfredsställande. Det gäller särskilt EDV och Hälso- och sjukvård.

Övervägande övriga incidenter har berott på handhavandefel av medarbetare. Nämnas kan att

- Genomförandeplaner lägg in i TES, vilket underlättar för mobil personal, men som rutinen säger inte får ske, utan dessa ska läsas i Treserva för att säkerställa korrekt uppdatering kring kunds hälsa för att minimera/eliminera risk för liv och hälsa.
- En personal tog av misstag bort alla planerade besök under en dag inom Hälso- och sjukvård.
- En personal har inte stängt journalen i Treserva samt att det finns ett känt fel, vilket gjorde att annan personal inte kom åt journalen.
- I och med rensning på O: upptäcks att fel och förmånga medarbetare har behörighet till en mapp de inte ska ha tillgång till.
- Brister i hanteringen av Siths-kort genom att låna ut kort till kollega som saknar kort samt lämnat kvar kort i dator vid arbetets slut.
- En risk för konfidentialiteten när en medarbetare ser att en annan medarbetare håller fram mobiltelefonen framför en sovande kund och misstänkte att kunden blev fotad.

Rekommendationer

Cybersäkerhetslagen (och CER)

Rekommendationen är som tidigare, att påbörja arbete med att analysera och planera för hur kommande krav i Cybersäkerhetslagen ska organiseras och genomföras inom sektorn. SG:s grupp med CISO, kommunjurist och IT-säkerhetsansvarig kommer att ge oss information löpande om VAD. Vi behöver påbörja ett arbete med HUR för att ha så mycket som möjligt på plats när lagen börjar gälla, troligen 1/8 2025.

Fas 4 i det systematiska informationssäkerhetsarbetet

Frågor kring uppföljning av genomförandet och dess effekt behöver tas fram och beslutas. ”Hur ska uppföljning av genomförande och dess effekt genomföras och vem har ansvaret?” Ansvaret för informationssäkerheten är Informationsägare. Rollen Informationsägare finns inte etableras på sektor Välfärd utan innehas av chef för aktuell verksamhet. Ansvaret är inte tydligt för respektive chef varför åtgärder inte genomförs.

Utbildningsplan

När Cybersäkerhetslagen träder i kraft kommer den att ange att utbildning är obligatorisk för verksamheternas ledningar/chefer samt att all personal ska erbjudas utbildning.

Organisation

Rekommendationen kvarstår enligt förslag från 2023 att etablera lokala stöd för chefer i rollen som Informationsägare, s.k. DISK:ar.

Genomförande av åtgärder

Eftersom endast hälften av föreslagna och godkända åtgärder faktiskt genomförs inom tidsperioden rekommenderas att dels förslag kring ansvar att följa upp tas fram, beslutas och etableras, dels att rollen Informationsägare etableras och Informationsägare får utbildning och information om vad som förväntas av dem. Om inte en ökning sker finns inte nyttan med allt arbete som görs för att identifiera risk för vår informationssäkerhet. ”Vi vet riskerna men vi bryr oss inte”.

Implementation av rutiner

Många rutiner har tagit fram för stöd till verksamheterna att arbeta informationssäkert och därmed skydda sin information. Men dessa rutiner är inte kända eller implementerade. Rekommendationen är att utarbeta ett arbetssätt för hur rutiner ska informeras och hur tillämpningen ska säkerställas.

Ledningarnas engagemang

Att driva, införa och stödja verksamhet med 3000 medarbetare och 100 chefer som har fullt upp med att leverera sina tjänster utan aktiva ledningar och nämnder har varit en stor utmaning och inte ett framgångsrikt vägval. Rekommendationen är att alla ledningsgrupper och nämnder prioriterar informationssäkerhet och dataskydd genom att frågorna finns på agendan, för beslut samt arbetar aktivt med införandet och tillämpningen så att vi ökar vår informationssäkerhet. Det skulle även ge ett behövligt stöd till samordnarna i arbetet med införandet av det systematiska informationssäkerhetsarbetet samt ge sektorn bra förutsättningar för att skydda informationen och kunders fri- och rättigheter, följa kommande lag och därmed undvika höga viten.

Plan för kommande år

Ingen plan finns för 2025 eftersom ISS kommer att sluta sin anställning.

Personliga rekommendationer

Nu när avslutar mitt uppdrag som informationssäkerhetssamordnare vill jag skicka med några rekommendationer som kommer från min upplevelse och reflektioner under mitt uppdrag. Rekommendationerna gynnar informationssäkerheten i hela sektor Välfärd och/eller underlättar min efterträdares arbetssituation.

Implementation av rutiner

Under åren har flera rutiner tagits fram av Informationssäkerhetssamordnare vars syfte är att öka informationssäkerheten. Tyvärr är rutinerna inte kommunicerade inom sektorn vilket innebär att förväntad effekt – ökad informationssäkerhet – uteblir. Frågan kring hur rutiner ska kommuniceras har lyft till kommunikationschef som skulle komma med ett förslag. En påminnelse har skett till

biträdande sektorchef. Ingen återkoppling har getts. Arbetet med att utarbeta rutiner känns därför onödigt eftersom förväntad effekt aldrig uppnåtts. Min rekommendation är att sektorn tar fram en kommunikationsstrategi som visar vem och hur nya rutiner ska implementeras och kommuniceras för att få förväntad effekt.

Upprättande av rutiner

Nytt arbetssätt infördes som innebar att innan en rutin upprättades skulle ledningsgruppen Utveckling och stöd godkänna förslaget. Trots att rutiner lämnats för godkännande så har ingen återkoppling skett till upprättaren. Min rekommendation är att ledningsgruppen ser över sitt arbetssätt i syfte att effektivisera processen. När jag som upprättare börjar på en rutin så har jag ofta klart för mig hur jag ska formulera rutinen så att den blir funktionell och förståelig. Får jag vänta månader på ett godkännande tappas tankar, syfte och motivation.

Tekniska informationssäkerhetskrav

Hittills har Informationssäkerhetssamordnare stämt av de tekniska informationssäkerhetskraven med IT Säkerhetsansvarig på SG vid genomförande av informationssäkerhetsklassningar. Informationssäkerhetssamordnare nu har identifierat att återkoppling från SG IT uteblir. Eftersom tekniken är ett centralt område inom informationssäkerhet behövs det tydliggöras hur bedömning ska genomföras. Min rekommendation är att Välfärd stämmer av med SG IT på vilket sätt bedömning av teknisk lösning är informationssäker.

Systematisk systemförvaltning

Arbetet med att öka informationssäkerheten har ett nära samband med systemförvaltning. För att få till ett gott samarbete behöver båda områdena arbeta systematiskt. Min rekommendation är att verksamhetsnära systemförvaltning Välfärd arbetar systematiskt kring alla IT-lösningar/informationsbärare (system, applikationer, nätverk, osv) som Välfärds nämnder ansvar för. Arbetet bör innefatta tvärfunktionella förvaltningsgrupper där även verksamhet och leverantör deltar i någon mån. Med systematiskt arbete avses beprövade metoder på marknaden.

Åtgärder i syfte att öka informationssäkerheten

Vid genomförande av riskanalys och vid incidenter uppkommer åtgärder som ska genomföras i syfte att öka informationssäkerheten. Ansvarig för genomförandet av åtgärderna är i huvudsak chef/Informationsägare. Många åtgärder blir inte genomförda vilket innebär att informationssäkerheten inte ökar och risken kvarstår. Behov finns därför att utse någon som dels kan följa upp föreslagna åtgärder, dels stödja åtgärdsansvariga i genomförandet av åtgärden.